IN THE CLAIMS:

The text of all pending claims are set forth below. Cancelled and withdrawn claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (previously amended), (cancelled), (withdrawn), (new), (previously added), (reinstated - formerly claim #), (previously reinstated), (re-presented - formerly dependent claim #) or, (previously re-presented).

Please AMEND the claims in accordance with the following:

1. (CURRENTLY AMENDED) An authentication system comprising:

a signing station which creates an authenticator by applying a one-way function to an information and then appends a signature generated from the authenticator to the information;

a certifying station for checking the authentication of the information from the authenticator included in ~~the~~ data received from said signing station;

wherein said signing station has,

a first authenticator creating unit for dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the divided data divided from the information to be signed; and

a linking unit for linking the plurality of authenticators created in said first authenticator creating unit to the respective divided data of the information from which the authenticators were created;

and wherein said certifying station has,

a separating unit for separating the information and the plurality of linked authenticators from the data received from said signing station;

a second authenticator creating unit for dividing the information separated by said separating unit into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a certifying unit for comparing the plurality of authenticators created by said

second authenticator creating unit with the plurality of authenticators separated from the information by said separating unit, and checking the authentication of the information.

2. (ORIGINAL) An authentication system according to Claim 1; wherein said linking unit links the authenticators obtained by truncating the authenticators created by said first authenticator creating unit to the information, and

said certifying unit compares the authenticators obtained by truncating the authenticators created by said second authenticator creating unit to the authenticators separated from the information by said separating unit and checking the authentication of the information.

3. (ORIGINAL) An authentication system according to Claim 2; wherein said first authenticator creating unit and said second authenticator creating unit create a first authenticator by subjecting a first data to a one-way operation using a first key, and prepare a second authenticator by subjecting a second data to a one-way operation using a second key.

a3

4. (CURRENTLY AMENDED) An authentication system according to Claim 3; wherein ~~each of~~

said first authenticator creating unit ~~and said second authenticator creating unit~~ discretely and independently creates the first authenticator and the second authenticator in parallel with each other, and

said second authenticator creating unit discretely and independently creates the first authenticator and the second authenticator in parallel with each other.

5. (ORIGINAL) An authentication system according to Claim 3; wherein each of said first authenticator creating unit and said second authenticator creating unit utilize an intermediate data when creating the second authenticator, which intermediate data is generated when the first authenticator is created.

6. (CURRENTLY AMENDED) An authentication method applied in an authentication system, wherein said authentication system has a signing station which creates an authenticator by applying a one-way function to an information and then appends a signature generated from

the authenticator to the information, and a certifying station for checking the authentication of the information from the authenticator included in ~~the~~ data received from said signing station; wherein

~~said~~ at the signing station, ~~executes,~~executing at least:

a first authenticator creating ~~step of~~ procedure dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the divided data divided from the information to be signed; and

a transmitting ~~step of~~ procedure linking the plurality of created authenticators created in said first authenticator creating ~~step~~ procedure to the respective divided data of the information from which the authenticators were created and transmitting the information to the certifying station; and

~~said~~ at the certifying station, executing at least: ~~executes,~~

a3

a separating ~~step of~~ procedure separating the information and the plurality of linked authenticators from the data received from said signing station;

a second authenticator creating ~~step of~~ procedure dividing the information separated in said separating ~~step~~ procedure into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a certifying ~~step of~~ procedure comparing the plurality of authenticators created in said second authenticator creating ~~step~~ procedure with the plurality of authenticators separated from the information in said separating ~~step~~procedure, and checking the authentication of the information.

7. (CURRENTLY AMENDED) An authentication method according to Claim 6; wherein said transmitting ~~step~~ procedure comprises a ~~step of~~ procedure linking the authenticators obtained by truncating the authenticators created in said first authenticator creating ~~step~~ procedure to the information, and

said certifying ~~step~~ procedure comprises a ~~step~~ procedure of comparing the authenticator obtained by truncating the authenticators created in said second authenticator creating ~~step~~ procedure to the authenticators separated from the information in said separating ~~step~~ procedure

and a ~~step of~~ procedure checking the authentication of the information.

8. (CURRENTLY AMENDED) An authentication method according to Claim 7; wherein said first authenticator creating ~~step~~ procedure and said second authenticator creating ~~step~~ procedure comprise a ~~step of~~ procedure creating a first authenticator by subjecting a first data to a one-way operation using a first key, and a ~~step of~~ procedure creating a second authenticator by subjecting a second data to a one-way operation using a second key.

9. (CURRENTLY AMENDED) An authentication method according to Claim 8; wherein ~~each of~~

said first authenticator creating procedure~~step and said second authenticator creating step comprise~~ comprises a ~~step of~~ procedure discretely and independently creating the first authenticator and the second authenticator in parallel with each other, and

said second authenticator creating procedure includes a procedure discretely and independently creating the first authenticator and the second authenticator in parallel with each other.

a3

10. (CURRENTLY AMENDED) An authentication system according to Claim 8; wherein each of said first authenticator creating ~~step~~ procedure and said second authenticator creating ~~step~~ procedure comprise a ~~step of~~ procedure utilizing an intermediate data when creating the second authenticator, ~~which~~where

intermediate data is generated when the first authenticator is created.

11. (CURRENTLY AMENDED) A computer-readable recording medium with a program recorded therein for making a computer execute the authentication method applied in an authentication system, wherein said authentication system has a signing station which creates an authenticator by applying a one-way function to an information and then appends a signature generated from the authenticator to the information, and a certifying station for checking the authentication of the information from the authenticator included in ~~the~~ data received from said signing station; wherein

the program makes said signing station execute at least,

a first authenticator creating ~~step of~~ procedure dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators.by applying a different one-way function to each of the divided data divided from the information to be signed; and

a transmitting ~~step of~~ procedure linking the plurality of authenticators created in said first authenticator creating ~~step~~ procedure to the information and transmitting the information to the certifying station; and

the program makes said certifying station execute at least,

a separating ~~step of~~ procedure separating the information and the plurality of linked authenticators from the data received from said signing station;

a second authenticator creating ~~step of~~ procedure dividing the information separated in said separating ~~step~~ procedure into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a certifying ~~step of~~ procedure comparing the plurality of authenticators created in said second authenticator creating ~~step~~ procedure with the plurality of authenticators separated from the information in said separating ~~step~~procedure, and checking the authentication of the information.

12. (CURRENTLY AMENDED) A signing apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information; said apparatus comprising:

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a linking unit for individually linking each authenticator of the plurality of created authenticators to the information.

13. (CURRENTLY AMENDED) A signing apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information; said apparatus comprising:

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied~~.~~; and

a linking unit for individually linking each authenticator of the plurality of created authenticators to the information.

14. (CURRENTLY AMENDED) A certifying apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information as well as checks the authentication of the information; said apparatus comprising:

a3

a separating unit for separating information and the plurality of authenticators from the data;

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for creating an authenticators by utilizing a key and applying a different one of a plurality of one-way functions corresponding to each of the divided data; and

a certifying unit for checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

15. (ORIGINAL) A certifying apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information as well as checks the authentication of the information; said apparatus comprising:

a separating unit for separating information and the plurality of authenticators from the data;

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

a certifying unit for checking the authentication of the information based on each of the

created authenticators and each of the separated authenticators.

16. (CURRENTLY AMENDED) A computer-readable recording medium with a program recorded therein for making a computer execute at least:

a dividing ~~step of~~ procedure dividing an information into a plurality of data;

an authenticator creating ~~step of~~ procedure creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a linking ~~step of~~ procedure individually linking each authenticator of the plurality of created authenticators to the information.

17. (CURRENTLY AMENDED) A computer-readable recording medium with a program recorded therein for making a computer execute at least:

a dividing ~~step of~~ procedure dividing an information into a plurality of data;

an authenticator creating ~~step of~~ procedure repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the--next data when the one-way function was applied; and

a linking ~~step of~~ procedure individually linking each of the plurality of created authenticators to the information.

18. (CURRENTLY AMENDED) A computer-readable recording medium with a program recorded therein for making a computer execute at least:

a separating ~~step of~~ procedure separating information and a plurality of authenticators from the data;

a dividing ~~step of~~ procedure dividing the information into a plurality of data;

an authenticator creating ~~step of~~ procedure creating an authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a certifying ~~step of~~ procedure checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

19. (CURRENTLY AMENDED) A computer-readable recording medium with a program recorded therein for making a computer execute at least:

a separating ~~step of~~ procedure separating information and plurality of authenticators from a data;

a dividing ~~step of~~ procedure dividing the information into a plurality of data;

an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

a certifying ~~step of~~ procedure checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

20. (CURRENTLY AMENDED) A signing method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information; said method comprising:

a3

a dividing ~~step of~~ procedure dividing an information into a plurality of data;

an authenticator creating ~~step of~~ procedure creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a linking ~~step of~~ procedure individually linking each authenticator of the plurality of created authenticators to the information.

21. (CURRENTLY AMENDED) A signing method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information; said method comprising:

a dividing ~~step of~~ procedure dividing an information into a plurality of data;

an authenticator creating ~~step of~~ procedure repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

a linking ~~step of~~ procedure individually linking each authenticator of the plurality of created authenticators to the information.

22. (CURRENTLY AMENDED) A certifying method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information as well as the authentication of the information is checked; said method comprising:

a separating ~~step of~~ procedure separating information and a plurality of authenticators from the data;

a dividing ~~step of~~ procedure dividing the information into a plurality of data;

an authenticator creating ~~step of~~ procedure creating an authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a certifying ~~step of~~ procedure checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

23. (CURRENTLY AMENDED) A certifying method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information as well as the authentication of the information is checked; said method comprising:

a3

a separating ~~step of~~ procedure separating information and plurality of authenticators from a data;

a dividing ~~step of~~ procedure dividing the information into a plurality of data;

an authenticator creating ~~step of~~ procedure repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

a certifying ~~step of~~ procedure checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

24. (NEW) An authentication system according to Claim 1, wherein said information is document data.

25. (NEW) An authentication system according to Claim 6, wherein said information is

document data.

a3

26. (NEW) An authentication system according to Claim 11; wherein said information is document data.